IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

Claims 1-7 (canceled).

8. (currently amended)A security management method for supporting security management of ~~each of~~ a plurality of managed systems executed in ~~constituting~~ an information system comprised of computers connected through a network~~with an electronic computer~~, comprising:

a security design ~~specification hatching~~ step for designing security specifications to be applied to the information system by ~~of~~ extracting an information security policy which corresponds to each managed system constituting an information system designated by a user from a database where ~~describing~~ a correspondence between information security policies representing policies of security measures with at least one managed system and said managed systems is described~~, to hatch security specifications to be applied to the information system~~;

a security ~~diagnosis~~ install step ~~of~~ for executing a plurality of audit programs wherein a process is described to audit ~~describing a processing for auditing various information including a type of the managed system and a software version, which are stored so as to correspond to each set of~~security status concerning the information security policy ~~and the managed system~~ which ~~are~~ is specified by security specifications ~~hatched~~ designed in said security ~~specification hatching~~design step~~, as well as by a security status to~~

~~audit the various information including the type and the software version of the managed system constituting the information system designated by the user, and to diagnose a security of said information system~~ for collecting the security status of each managed system designated by the user, and for changing the security status of the managed systems designated by the user, based on the collected information, in consistency of information security policies specified by security specifications designed in said security design step; and

a security ~~handling and~~ management step ~~of~~for executing the install step periodically~~a management program designated by the user, from a plurality of management programs describing a process for controlling the security status concerning the information security policy of the managed system, stored so as to correspond to each set of the information security policy and the managed system which are specified by the security specifications hatched in said security specification hatching step, to allow said electronic computer to change the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program~~.

9. (currently amended) The security management method according to claim 8, wherein ~~in~~ said security ~~diagnosis~~ install step comprises:~~,~~

a diagnosis step for diagnosing the security of the information system designated by said user by extracting the audit program made to correspond to each set of the information security policy and the managed system, which are specified by the security specifications ~~hatched~~ designed in said security specification ~~hatching~~ design step, ~~is extracted~~ from a database ~~describing~~ where a correspondence is described of the information security policy, the managed system and the audit program where a process is written to audit ~~describing a processing for auditing various information such as the type and the software version of said managed system as well as the~~ security status concerning said information security policy of said managed system, and executing~~executed, to diagnose the security of the information system designated by said user~~; and

~~in said security handling and management~~a change step, wherein the management programs, made to correspond to each set of the information security policy and the managed system, which are specified by the security specifications ~~hatched~~ designed in said security specification ~~hatching~~ design step, are extracted from a database describing a correspondence of the information security policy, the managed system and the management program describing a processing for controlling the security status concerning the security policy, the managed system and said information security policy of a security of said managed system, and the management program designated by the user is extracted among the extracted programs to be executed, to allow the security status of the managed system corresponding

to the extracted management program to adjust to the information security policy corresponding to the management program.

Claim 10 (canceled).

11. (previously presented) The security management method according to claim 8, wherein in accordance with a security setting content received from the user, said management program changes the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program.

12. (previously presented) The security management method according to claim 8, wherein a security hole information published by a security information organization including CERT or Computer Emergency Response Team and diagnosis results obtained in said security diagnose step which is executed for the information system designated by the user are reflected in the database describing the correspondence of the information security policy with at least one managed system and said audit/management program stored so as to correspond to each set of the information security policy and the managed system.

13. (currently amended)A security management system for supporting security management of managed systems executed in ~~constituting~~ an information system comprised of computers connected through a network, comprising:

~~a database describing a correspondence between information security policies representing a policy of a security measure with at least one managed system and said managed systems;~~

~~a security specification hatching section for extracting an information security policy which corresponds to each of the managed systems constituting the information system designated by a user from said database, to hatch security specifications to be applied to the information system;~~

~~a plurality of audit sections for auditing various information including a type and a software version of the managed system as well as a security status concerning the information security policy of the managed system, each audit section being provided so as to correspond to each set of the information security policy and the managed system, which are specified by security specifications hatched by said security specification hatching section;~~

~~a security diagnosis section for diagnosing a security of the information system designated by said user based on the diagnosis results in each of said audit sections;~~

~~a plurality of management sections for controlling a security status concerning the information security policy of the managed system, each management section being provided so as to correspond to each set of the~~

~~information security policy and the managed system, which are specified by security specifications hatched by said security specification hatching step;~~

~~a security handling and management section for executing a management section designated by said user to change the security status of the managed system corresponding to the management section so as to adjust the security status to the information security policy corresponding to the management section.~~

a storage device which stores first database for storing the information specifying the managed systems, being a subject to which information security policies are applied;

second database for storing the information specifying the specifications of information security policy; and

third database wherein correspondence between the managed systems and information security policies is described;

a management and audit object area control section which extracts, from said first database managed systems being a subject to which information security polices are applied due to a designation by a user;

an information security policy selection control section which extracts, from said second database, information security policy specifications due to a designation by a user;

an information security policy/security management and audit program correspondence control section which extracts, from said third database, information security policy corresponding to the managed systems selected in said management and audit object area control section, specifies the

specification corresponding to the extracted information security policy among the specifications selected in said information security policy selection control section, and designs specification of the information security policies for each of the managed system;

a plurality of audit sections which audit security status concerning the information security policy which is specified by security specifications designed in an information security policy/security management and audit program correspondence control section;

a plurality of management sections which collect the security status of the information system designated by the user based on the audit results from the plurality of audit sections and control security status concerning the information security policy of the managed systems in order to bring the security status of the managed systems designated by the user in conformity with the information security policy specified by the security specification designed at the information security policy/security management and audit program correspondence control section based on the collected information,

wherein the information security policy/security management and audit program correspondence control section has the process at the audit modules and management modules executed periodically.